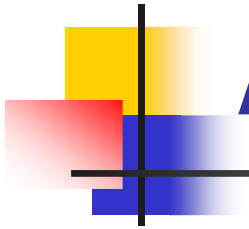
RACF Power Tools – Using IRRICE and Rexx on IRRADU00 and IRRDBU00 Part 1

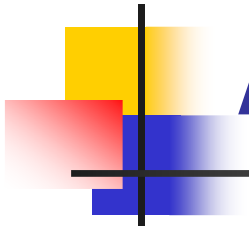
NewEra Software - The z Exchange
June 10, 2015

Thomas Conley
Pinnacle Consulting Group, Inc.
59 Applewood Drive
Rochester, NY 14612-3501
P: (585)720-0012
F: (585)723-3713
pinncons@rochester.rr.com



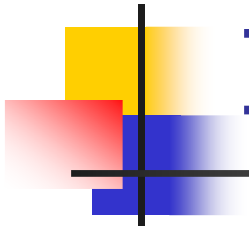
Abstract

Do you need to audit a RACF environment? Do you need to figure out who is doing what to whom? Are you one step away from a failed PCI/HIPAA/SOX/DISA audit? If you answered yes to any of these questions, then this session is for you! Come to this session to learn about IRRADU00 and IRRDBU00, and how to use IRRICE and Rexx to extract the data you need. This session is designed for skill levels from beginners to experts.



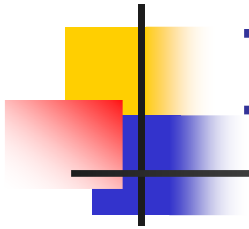
Agenda

- IRRADU00
- IRRDBU00
- IRRICE
- Summary
- Finally…



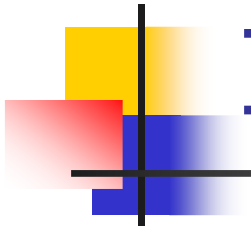
IRRADU00

- IRRADU00 is RACF's audit utility
- Extract RACF-related SMF record data
- Utility is actually a set of exits that plug into SMF dump program IFASMFDP
- Creates flat file or XML file of records describing RACF activity, for input into other processes
- Can be processed by ICETOOL, Rexx, uploaded into DB2 and queried with SYS1.SAMPLIB members IRRADULD, IRRADUTB, IRRADUQR, etc.



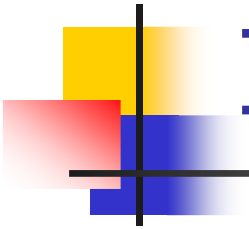
IRRADU00

- IRRADU00 fully documented in RACF Auditor's Guide
- IRRADU00 holds critical information about your system controls, so only the most trusted users on the system should have access to that data
- IRRADU00 extracts following SMF records:
  - Type 30
    - Subtype 1 - Job initiation
    - Subtype 5 - Job termination
  - Type 80 - Resource access (no subtypes)



IRRADU00

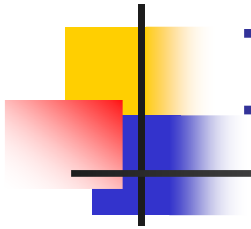
- IRRADU00 extracts following SMF records (cont'd):
  - Type 81 - RACF initialization (no subtypes)
  - Type 83
    - Subtype 1 - Data sets affected by a security label change
    - Subtype 2 - EIM
    - Subtype 3 - LDAP
    - Subtype 4 - Remote audit
    - Subtype 5 - Websphere
    - Subtype 6 - TKLM



IRRADU00

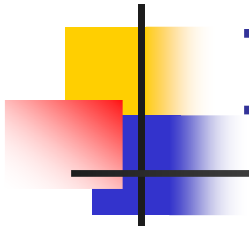
- IRRADU00 JCL:

```
//SMFUNLD JOB ,'SMF DATA UNLOAD',
//          MSGLEVEL=(1,1)
//SMFDUMP  EXEC PGM=IFASMFDP
//SYSPRINT DD SYSOUT=A
//ADUPRINT DD SYSOUT=A
//OUTDD    DD DISP=SHR,DSN=TCONLEY.RACF.IRRADU00
//SMFDATA  DD DISP=SHR,DSN=TCONLEY.RACF.SMFDATA
//*XMLFORM DD  DUMMY   **Use this or XMLOUT for XML output
//*XMLOUT  DD  DUMMY
//SMFOUT   DD DUMMY
//SYSIN    DD *
 INDD(SMFDATA,OPTIONS(DUMP))
 OUTDD(SMFOUT,TYPE(000:255))
 ABEND(NORETRY)
 USER2(IRRADU00)
 USER3(IRRADU86)
/*
```



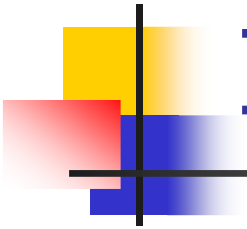
IRRADU00

- OUTDD is a variable-length LRECL(8192) file
- IRRADU00 will change LRECL to 8192
- Can also create XML output using DD's XMLFORM or XMLOUT (compressed XML)
- IRRADU00 creates output based on this priority:
  - XMLFORM
  - XMLOUT
  - OUTDD
- IRRADU00 creates only one of above outputs



IRRDBU00

- IRRDBU00 is RACF's database unload utility
- RACF profiles are extracted into flat file format
- Many record types describing users, groups, profiles, access lists, connections, etc.
- Armed with an IRRDBU00 file, anyone will know EXACTLY what your RACF environment looks like, and where to find holes
- Only most trusted personnel should have access to IRRDBU00 or file created by it

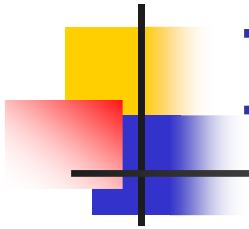


IRRDBU00

- IRRDBU00 JCL:

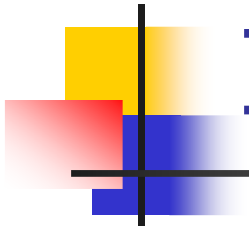
```
//USER01 JOB Job card...
//UNLOAD EXEC PGM=IRRDBU00,PARM=NOLOCKINPUT
//SYSPRINT DD SYSOUT=*
//INDD1    DD DISP=SHR,DSN=SYS1.RACFDB.PART1.COPY
//INDD2    DD DISP=SHR,DSN=SYS1.RACFDB.PART2.COPY
//OUTDD    DD DISP=SHR,DSN=TCONLEY.RACFDB.IRRDBU00
```

- INDDx are RACF database splits, INDD1 if not
- OUTDD holds unloaded RACF database
- OUTDD is VB with LRECL >= 4096



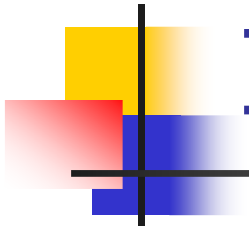
IRRDBU00

- Run against RACF DB copy, with NOLOCKINPUT
- Can run against following datasets, in ascending order by system impact
  - Backup copy of RACF database
  - Backup RACF database
  - Primary RACF database
- If running against active RACF database, use LOCKINPUT to ensure unload file integrity, and review RACF Security Admin Guide for impacts



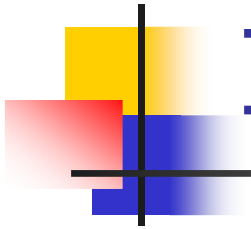
IRRDBU00

- IRRDBU00 will analyze and detect errors in RACF structures
- If errors found, can be corrected with IRRUT200, BLKUPD, or other tools
- IRRDBU00 is only way to list all members of universal groups, especially universal groups exceeding LISTGRP display limit



IRRICE

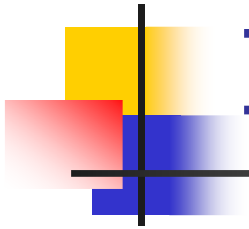
- IRRICE is set of canned reports running ICETOOL against IRRADU00 and IRRDBU00
- SYS1.SAMPLIB(IRRICE) is an IEBUPDTE SYSIN to create PDS of reports, control members, and procs
- Easy to install and run
- 75-90% of RACF data required to audit environment will be found in IRRICE reports



IRRICE

- Install IRRICE with this job:

```
//IBMUSERR  JOB (CONLEY),' RACF BATCH ',CLASS=A,
//             MSGCLASS=H,NOTIFY=&SYSUID
//*******************************************************
//IRRICE   EXEC PGM=IEBUPDTE,PARM='NEW'
//SYSPRINT DD SYSOUT=*
//SYSUT2   DD DSN=IBMUSER.IRRICE,
//            DISP=(NEW,CATLG,DELETE),
//            UNIT=SYSALLDA,
//            SPACE=(CYL,(1,1,45)),
//            DCB=(DSORG=PO,RECFM=FB,LRECL=80,BLKSIZE=0)
//SYSIN    DD DISP=SHR,DSN=SYS1.SAMPLIB(IRRICE)
/*
```



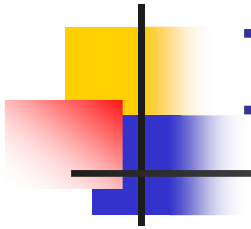
IRRICE

- Each IRRICE report designated by 4-byte id
- Each IRRICE report defined by pair of members in IRRICE PDS
  - xxxx is report name and contains ICETOOL control cards with report headers (e.g. OPER for report of accesses allowed by OPERATIONS attribute)
  - xxxxCNTL contains SORT control cards and selection criteria (e.g. OPERCNTL)

IRRICE

- Member OPER:

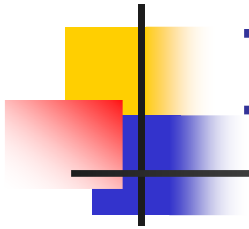
```
/*****************************************************************
* Name: OPER                                                     *
* Find all of the resource accesses that were allowed due to     *
* the user ID having the OPERATIONS attribute.                   *
*****************************************************************
 SORT    FROM(ADUDATA) TO(TEMP0001) USING(RACF)
 DISPLAY FROM(TEMP0001) LIST(PRINT) -
         PAGE -
         TITLE('OPER: Accesses Allowed Because of OPERATIONS') -
         DATE(YMD/) -
         TIME(12:)  -
         BLANK -
         ON(23,8,CH)   HEADER('Time') -
         ON(32,10,CH)  HEADER('Date') -
         ON(63,8,CH)   HEADER('User ID') -
         ON(286,36,CH) HEADER('Resource Name') -
         ON(564,6,CH)  HEADER('Volume') -
         ON(605,36,CH) HEADER('Profile')
```



IRRICE

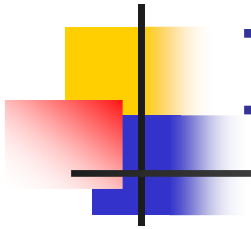
- Member OPERCNTL:

```
SORT    FIELDS=(63,8,CH,A)
INCLUDE COND=(5,8,CH,EQ,C'ACCESS',AND,
              91,3,CH,EQ,C'YES')
OPTION  VLSHRT
```



IRRICE

- Other members in IRRICE PDS:
  - $$CNTL$$ - Main JCL for all xxxx reports, invokes RACFICE proc
  - $CFQG – example using OUTFIL construct to report on HLQ's with > 100 fully-qualified generic profiles
  - $CHLQ – example using OUTFIL construct to report on HLQ's with > 200 generic profiles
  - $ULAST90 – example with embedded Rexx exec to report on user profiles created within last 90 days
  - RACFICE – main JCL proc for all xxxx reports



IRRICE

- After populating IRRICE PDS, customize member $$CNTL$$ for your installation
  - Jobcard
  - Scroll down and modify JCLLIB and SET statements:

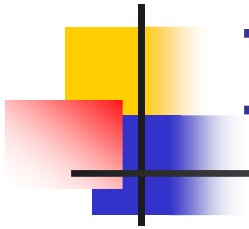
```
JCLLIB ORDER=<IRRICE PDS>
SET  ADUDATA=<IRRADU00 dataset>
SET  DBUDATA=<IRRDBU00 dataset>
SET  ICECNTL=<IRRICE PDS>
```

- Update RACFICE member for SORT messages

```
//DFSMSG    DD SYSOUT=*
```

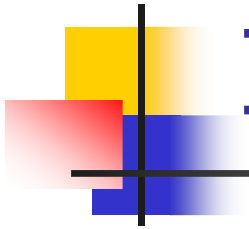
IRRICE

- $$CNTL$$ JCL member can now run to create reports
- To avoid errors in SORT, IRRICE and IRRDBU00 should be at same software level
- Reports of general interest to auditors italicized



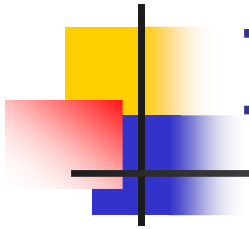
IRRICE

- IRRICE creates these reports from IRRADU00:
  - ACD$ - Users using automatic command direction
  - CADU - Count of IRRADU00 events
  - CCMD - Count of commands issued (by user)
  - ECD$ - Users who are directing commands explicitly
  - LOGB - Users who log on with LOGON BY
  - *LOGF - All users with excessive incorrect passwords*
  - *OPER - Accesses allowed because user has OPERATIONS authority*
  - PWD$ - Users using password synchronization



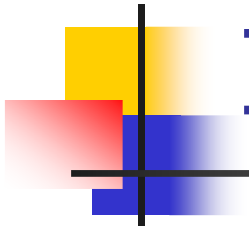
IRRICE

- IRRICE creates these reports from IRRADU00:
  - RACL - RACLINK audit records
  - RINC - RACF class initialization records
  - *SELU - All audit records for a specific user*
  - *SPEC - Events that succeeded because user has SPECIAL authority*
  - *TRMF - Excessive incorrect passwords from terminals*
  - *VIOL - Access violations*
  - *WARN - Accesses allowed due to WARNING mode profiles*



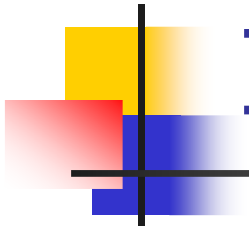
IRRICE

- IRRICE creates these reports from IRRDBU00:
  - *ALDS - Discrete data set profiles with IDs on access list with ALTER authority*
  - ASOC - Users with explicit associations defined
  - *BGGR - Discrete general resource profiles with generic characters in their name*
  - CCON - Count of user connections, flagging those with more than "x" (default 100) connections
  - CGEN - Count of general resource profiles
  - CPRO - Count of all RACF profiles



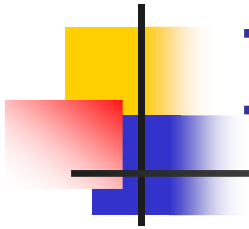
IRRICE

- IRRICE creates these reports from IRRDBU00:
  - *CONN - User IDs with group privileges above use*
  - GIDS - Shared UNIX System Services GIDs
  - *IDSC - Data set conditional access lists with ID(*) and access > NONE*
  - *IDSS - Data set standard access lists with ID(*) and access > NONE*
  - *IGRC - General resource conditional access lists with ID(*) and access > NONE*



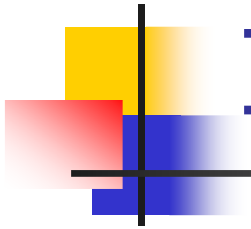
IRRICE

- IRRICE creates these reports from IRRDBU00:
  - *IGRS - General resource standard access lists with ID(*) and access > NONE*
  - OMVS - User IDs with OMVS segments
  - *PCAM - PROGRAM class specific profiles with MAIN or BASIC APPLDATA*
  - *SUPU - UNIX System Services superusers with UID(0)*
  - *UGLB - User IDs With extraordinary system-level authorities (SPECIAL, OPERATIONS, AUDITOR)*



IRRICE

- IRRICE creates these reports from IRRDBU00:
  - *UGRP - User IDs with extraordinary RACF group authorities (Group-SPECIAL, Group-OPERATIONS, Group-AUDITOR)*
  - *UIDS - Shared UNIX System Services UIDs*
  - *URVK - User IDs which are currently revoked*
  - *UADS - Data set profiles with UACC > NONE*
  - *UAGR - General resource profiles with UACC > NONE*
  - *WNDS - Data set profiles in WARNING mode*
  - *WNGR - General resource profiles in WARNING mode*

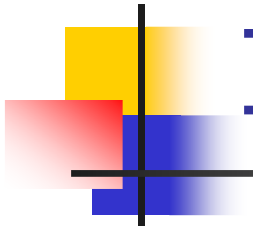


IRRICE

- Example of IRRADU00 report OPER (modified to fit):

```
- 1 -        OPER: Accesses Allowed Because of OPERATIONS        17/07/08        05:37:28 pm

Time       Date         User ID    Resource Name                          Volume   Profile
--------   ----------   --------   ------------------------------------   ------   -----------
00:15:00   2012-04-16   TCONLEY    PINNACLE.RACF.PROCLIB                  PINN01   PINNACLE.**
00:15:01   2012-04-16   TCONLEY    PINNACLE.RACF.CLIST                    PINN02   PINNACLE.**
```

- What's missing in this report?

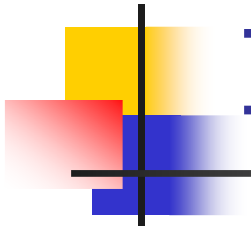


IRRICE

- Example of IRRADU00 report VIOL (modified to fit):

```
- 1 -        VIOL: Access Violations        17/07/08        05:37:49 pm

Date        Time      Result    User ID   Resource Name              Class     Volume  Profile
----------  --------  --------  --------  -------------------------  --------  ------  -----------
2012-04-16  18:33:05  INSAUTH   TCONLEY   MASTER.SYSACAT             DATASET   MCATV1  MASTER.*.**
```

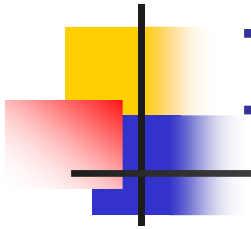
- What's missing in this report?



IRRICE

- Example of IRRDBU00 report UGBL:

```
- 1 -          UGLB: Users with Extraordinary Authorities

User ID    User Name                 Special   Operations   Auditor
--------   ---------------------     -------   ----------   -------
DSMON      DSMON                     YES       NO           NO
SYSPGTC    THOMAS CONLEY             YES       YES          YES
ZOPS       PRODUCTION ID             NO        YES          NO
```

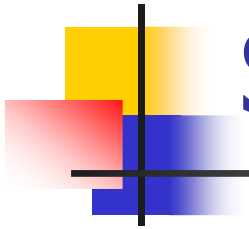


IRRICE

- Example of IRRDBU00 report URVK:

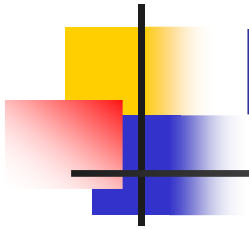
```
- 1 -          URVK: User IDs Which are Currently Revoked

User ID     User Name
--------    --------------------
irrcerta    CERTAUTH Anchor
irrmulti    Criteria Anchor
irrsitec    SITE Anchor
SORYBUT     USER WE FIRED AGES AGO
```

- What's missing in this report?



Summary

- Discussed IRRADU00 and IRRDBU00
- Showed how to install IRRICE and use it



Finally….

- I’m always interested to hear about your experiences with RACF, IRRADU00, IRRDBU00, and IRRICE, so if you have questions or come up with a neat solution to a problem, drop me an Email pinncons@rochester.rr.com